Customer No. 24498
Attorney Docket: RCA88783
Final Office Action Date: 03/03/2008

REMARKS

This application has been reviewed in light of the Office Action dated March 3, 2008. Claims 3, 4, 8 and 9 are pending in the application. By the present Amendment, claim 3 has been amended. Claims 1, 2 and 5-7 have been cancelled without prejudice. No new matter has been introduced. The Examiner's reconsideration of the rejection in view of the amendment and the following remarks is respectfully requested.

ALLOWABLE CLAIMS:

Applicant gratefully acknowledges the Examiner's indication that claims 3, 4, 8 and 9 would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Accordingly, Applicant has amended claim 3 to be rewritten in independent form to include the elements of claims 1 and 2. Therefore, claim 3 is now believed to be in condition for allowance. Claims 4, 8 and 9 depend from claim 3. The dependent claims include the limitations of claim 3 and are thus believed to be allowable. Claims 1, 2 and 5-7 have been cancelled, thus this application is now believed to be in condition for allowance.

103 REJECTIONS

By the Office Action, claim 1 stands rejected under 35 U.S.C. §103(a) as being unpatentable over by U.S. Patent No. 5,351,294 to Matsumoto et al. (hereinafter Matsumoto) in view of U.S. Patent No. 5,103,479 to Takaragi et al. (hereinafter Takaragi) and in view of U.S. Patent No. 5,737,424 to Elteto et al. (hereinafter Elteto).

Claim 2 was rejected under 35 U.S.C 103(a) as being unpatentable over Matsumoto et al. in view of Takaragi and in view of Elteto and in view of U.S. Patent No. 6,760,445 to Schwenk et al. (hereinafter Schwenk).

Applicant respectfully asserts that Matsumoto, Takaragi, Elteto and/or Schwenk either individually or in any combination, fail to disclose or suggest at least receiving, in said smart card, data representative of a first seed value, the first seed value representing a first point in a coordinate system; generating, in said smart card, said scrambling key using said first seed value and a second seed value in a predetermined function, the second seed value representing a second point in the coordinate system, whereby secret sharing is implemented, said second seed value being permanently stored in said smart card; and descrambling, in said smart card, said signal using said generated scrambling key to provide a descrambled signal.

In the present invention, the first seed value is supplied by a service provider and the second seed value is permanently stored in the smart card. Advantageously, this approach permits more than one service provider to share the stored second seed value, and each service provider is free to choose its own first seed value. The present claim elements and the flexibility provided thereby are not taught or suggested by the cited combination.

Matsumoto includes a **limited** broadcast system which must know which of the receiver stations are permitted to decrypt the encrypted data. The destination information (I) includes a string of 1's and 0's that indicate which receiver stations have permission to decrypt the data stream and which do not. This presupposes that each received station must be known by the information service provider 104 before a transmission is made. Matsumoto's method is only useful for limited broadcasts due at least to this limitation. While a secure system may be achieved by Matsumoto, the system does not provide the flexibility afforded by the method in accordance with the present invention.

Furthermore, Matsumoto does not disclose or suggest a second seed value being permanently stored in the smart card, essentially as claimed in claim 1. Instead, Matsumoto provides a computed k value that is determined based upon a present time that is read when the encrypted data is received (*see* col. 6, lines 27-30). While the IC card of Matsumoto includes a hash function, the hash function is a sum check that computes the cipher key K based on the parameter k and the number of blocks of the destination information. This is a dynamic computation that is only based on the information sent to the card. A permanent second seed in accordance with the present claims is not computed nor stored on a smart card.

The Examiner has cited Takaragi to cure the deficiencies of Matsumoto. However, even assuming *arguendo* that they could be combined, Takaragi fails to cure these deficiencies. Takaragi is directed to an encipher/decipher method which employs a smart card to supply keys for a high speed computational method. The smart card (112) stores keys (e.g., K_1 to K_4) to be introduced to the encipher/decipher equipment 100.

At col. 16, lines 25-32, Takaragi describes that the smart card may include a microcontroller to substitute for the CPU 110 of equipment 100. The Examiner cites this portion of Takaragi to teach that scrambling operations may be performed on a smart card. While such processing may, *arguendo*, be performed on the smart card, Takaragi fails to teach or suggest at least: receiving, in said smart card, data representative of a first seed value, the first seed value representing a first point in a coordinate system; generating, in said smart card, said scrambling key using said first seed value and a second seed value in a predetermined function, the second seed value representing a second point in the coordinate system, whereby secret sharing is implemented, said second seed value being permanently stored in said smart card. In Takaragi, keys are stored only on the smart card, whether the

smart card is only a card or includes a processor. Further, Takaragi makes no mention of two different seed values obtained from different sources and used to reconstruct an encryption key, as in the present invention.

Elteto, assuming *arguendo* that it could be combined with Matsumoto and/or Takaragi, fails to cure their deficiencies. Elteto refers to a method for encrypting messages using families of elliptic curves and generally mentions points on an elliptic curve system being used for encrypting and decrypting. However, Elteto is silent with respect to any teaching or suggestion of smart cards, much less generating in a smart card a scrambling key using a first and a second seed value, the first seed value being received by the smart card and the second seed value being permanently stored in the smart card.

Nevertheless, in the interest of furthering prosecution of this application, claims 1 and 2 have been cancelled without prejudice. Claim 3 has been amended to include the elements of claims 1 and 2, as discussed above. Claims 4, 8 and 9 depend from claim 3, which was deemed allowable.

Applicant respectfully reserves the right to file a continuation application during pendency of the present application, to cover a broader interpretation of the allowed claims.

Accordingly, the Applicants respectfully request withdrawal of all the rejections under 35 U.S.C. §103, and allowance of pending claims 3, 4, 8 and 9.

In view of the foregoing amendments and remarks, it is respectfully submitted that all the claims now pending in the application are in condition for allowance.

Customer No. 24498
Attorney Docket: RCA88783
Final Office Action Date: 03/03/2008

CONCLUSION

In view of the foregoing amendments and remarks, it is respectfully submitted that all the claims now pending in the application are in condition for allowance. Early and favorable reconsideration of the case is respectfully requested.

It is believed that no additional fees or charges are currently due. However, in the event that any additional fees or charges are required at this time in connection with the application, they may be charged to applicant's Deposit Account No. 07-0832.

Respectfully submitted,

Dated: January 6, 2009

By: _____
Paul Kiel
Registration No. 40,677

Mailing Address:

Patent Operations
Thomson Licensing LLC
P.O. Box 5312
Princeton, NJ 08543-5312

(609) 734-6815